LAWFARE
HARD NATIONAL SECURITY CHOICES

SECURITY BY DESIGN

Software Liability and Insurance

Daniel W. Woods* May 2024

Insurers can bring unique evidence and legal strategies to software liability cases if the regime creates a path for subrogation.

1. INTRODUCTION

Holding software vendors liable for bugs and security failures is a perennial public policy proposal.[1] This debate was animated by the 2023 U.S. National Cybersecurity Strategy, which observes that "too many vendors ignore best practices."[2] The strategy argues that public policy should "shift liability onto those entities that fail to take reasonable precautions to secure their software." Scholars are already asking traditional legal questions like whether the liability regime should be based on a negligence standard or a defect model imported from products liability, and how to define the standard of care.[3]

This paper explores how the policy regime should interact with the insurance industry. Insurance has the potential to both thwart and support the policy goals that motivate introducing a software liability regime. On the one hand, the goal of improving software security can be thwarted if vendors simply transfer the costs to an insurer without changing software development practices, an example of moral hazard. This is a potential concern because existing insurance products function to shield vendors from liability. Some firms

*Daniel Woods is a Lecturer in Cyber Security at the University of Edinburgh. His academic position is jointly appointed by the British University in Dubai, where he periodically teaches and supervises students. He received his PhD titled "The Economics of Cyber Risk Transfer" in 2019 from the University of Oxford. Daniel is also a Security Researcher at Coalition, a cyber insurance and security services start-up.

[1] Michael C. Gemignani, "Product Liability and Software," *Rutgers Computer & Technology Law Journal* 8 (1980): 173; Ross J. Anderson, "Liability and Computer Security: Nine Principles," in *European Symposium on Research in Computer Security* (Springer, 1994), 231–45; Daniel J. Ryan and C. Heckman, "Two Views on Security Software Liability. Let the Legal System Decide," *IEEE Security & Privacy* 1, no. 1 (2003): 70–72; Terrence August and Tunay I. Tunca, "Who Should Be Responsible for Software Security? A Comparative Analysis of Liability Policies in Network Environments," *Management Science* 57, no. 5 (2011): 934–59.

[2] The White House, *National Cybersecurity Strategy*, March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-CybersecurityStrategy-2023.pdf.

[3] Chinmayi Sharma and Benjamin C. Zipursky, "Who's Afraid of Products Liability? Cybersecurity and the Defect Model," *Lawfare,* Oct. 19, 2023; Jim Dempsey, "Standards for Software Liability: Focus on the Product for Liability, Focus on the Process for Safe Harbor," *Lawfare Security by Design Paper Series* (2024).

purchase liability insurance (known as Tech E&O) that covers errors and omissions in the provision of technology products and services.

On the other hand, insurance can support public policy. The goal of compensating victims of insecure software is supported when liability insurance provides a reliable source of recovery for victims of cyber incidents. Similarly, many businesses already buy cyber insurance that covers costs resulting from cybersecurity incidents. Insurance also provides certainty to vendors in managing litigation risk, which helps vendors to navigate future liability claims.[4] Insurers can also, in certain circumstances, help vendors to reduce liability risk by guiding them toward more secure development processes.

Unlike the previous examples that place insurance on the periphery of the liability regime, insurers can also act as prime movers within the liability regime. This can be shown with a hypothetical example. Suppose a cyber insurance policyholder, a hospital, suffers a ransomware incident in which the threat actor exploited how an internet-facing software solution authenticates users. The hospital's incident costs would be offset by an indemnity payment from the cyber insurer, but the vendor that built the software would most likely avoid liability for such costs even though they were responsible for building secure software.[5] This assignment of liability bristles with concepts of justice and accountability. The U.S. legal system seeks to assign responsibility for costs to the party whose negligence caused the accident. But even if legal reform created a route to assigning liability to the vendor, the insurer would already have compensated the victim.

To address this problem, insurers should be able to step into the shoes of the hospital and seek redress from the software vendor that was responsible for the incident. In the language of insurance law, the insurer should be able to *subrogate* against the vendor. Although it appears subrogation serves the interests of the insurer alone, it actually upholds two equitable principles. The first is to hold wrongdoers accountable for their wrongs. Subrogation means the party that is responsible for causing the loss pays a cost. The second benefit is upholding the indemnity principle, which says that a victim should not be better off after suffering a loss (as this could create perverse incentives). Absent subrogation, a policyholder could in theory recover from both their insurer and the wrongdoer, known as double recovery. With subrogation, the insurer receives the share of the monetary award, recovered from the wrongdoer, that was already paid out as an indemnity payment to the insured.

To further highlight the importance of insurers within the liability regime, consider that insurers also defend potentially liable parties that have purchased liability insurance. Liability insurance

[4] The safe harbor is introduced to provide vendors with financial certainty. The White House, *National Cybersecurity Strategy.*

[5] The precise contours of this argument are an open question. We cannot expect vendors to build flawless software, which is not possible even with state-of-the-art development practices. However, this proposal assumes an established rationale for when vendors should be held liable, or at least that one could be developed by case law.

policies transfer rights to the insurer to defend the private action on the policyholder's behalf. Given that insurers find themselves on both sides of liability claims, the industry's meta incentive is to create an efficient system that resolves liability claims while minimizing legal costs.

These links between liability and insurance are not unique to software. Kenneth Abraham paints a history of the twentieth century in which insurance is at the center of the expansion of liability.[6] Plaintiffs sought compensation for injuries covered by liability insurance, as it provided a reliable source of recovery. To control the costs, insurers began to step between "injurer and victim," predominantly by defending the liable party but also by using subrogation rights to seek compensation on behalf of the injured first-party. Over time, the two systems became intertwined in such a way that "tort becomes insurance, and insurance becomes tort."[7] This led Abraham to describe insurance and the tort system as "two suns in a binary star, dependent on each other for their position in our legal system."

To anticipate the interaction between software liability and insurance—the other sun in Abraham's binary star—this paper explores how to design a policy regime with insurance in mind. We argue that insurers can make a unique contribution to enforcing and administering the liability regime.[8] This article's proposal consists of pro-subrogation measures that enable insurers to pursue vendors and recover claims paid out to victims of security incidents. This system provides victims with rapid compensation via insurance without dulling the regime's ability to deter insecure software development.

It is perhaps unusual to call for pro-subrogation policy.[9] Nevertheless, there are historical precedents for legislation that encourages subrogation motivated by public policy goals, such as to reduce the cost of Medicare.[10] In the case of software liability, the motivation is that private actions brought by insurers will strengthen accountability under the liability regime. To the extent there is not enough software insecurity litigation as argued in the 2023 National Cybersecurity Strategy,[11] pro-subrogation measures can address the problem.[12]

---

[6] Kenneth S. Abraham, *The Liability Century: Insurance and Tort Law From the Progressive Era to 9/11* (Harvard University Press, 2008).

[7] Ibid.

[8] We acknowledge that insurers will sometimes opt against enforcing their subrogation rights for commercial reasons that we unpack in Section 4. Even so, insurers can be powerful litigants in the actions they do pursue via subrogation.

[9] The rules around subrogation developed mostly through case law, with specific rules varying by state and insurance line. For example, Parker notes that "life insurance is generally viewed as an investment contract to which the principle of subrogation is rarely, if ever, applied." Johnny C. Parker, "The Made Whole Doctrine: Unraveling the Enigma Wrapped in the Mystery of Insurance Subrogation," *Missouri Law Review* 70 (2005): 723.

[10] Sally Hart, "The Myth of the Superlien: Medicare Secondary Payer Law Clarified," *NAELA Journal* 5 (2009): 95–104.

[11] The White House, *National Cybersecurity Strategy*.

[12] Admittedly, this could change in the future, which may justify reversing the pro-subrogation measures or even introducing anti-subrogation measures.

Additional pro-subrogation arguments can be found in cost-efficiency and the insurers' access to private information. The cost-efficiency of insurers in administering liability claims applies to all lines of insurance. Whereas class-action lawyers face incentives to inflate legal costs as they are a law firm's main source of revenue, insurers face incentives to reduce legal costs as they show up as a cost item on insurers' balance sheets. Insurers can also build legal strategies that economize on scale—insurers employ teams of attorneys to craft and implement legal strategies, and exploit long-term benefits, given that a legal case that establishes precedent could be used to recover on behalf of future policyholders.

The informational advantage is especially profound for cyber risk. In the science of cybersecurity, there is little public evidence about which software solutions or development methodologies are associated with less risk, let alone whether there is a causal relationship.[13] In contrast, insurers have started to publicly report on correlational evidence that certain software solutions are associated with significantly higher risk.[14] This kind of actuarial evidence could inform a liability claim against a vendor and also quantify several liability in the event a vendor is held only partially liable.

The aforementioned combination of a lack of litigation, cost-efficiency, and insurers' private information motivate the pro-subrogation measures in the proposal. Box 1 provides a concise overview of this article's proposal. Section 2 describes the rationale behind the proposal. Section 3 anticipates how this proposal will impact different stakeholders. Section 4 concludes the paper.

Box 1: Pro–Cyber Subrogation Measures

Each measure strengthens the rights of insurers in subrogating against software vendors. In practice, lawmakers need to calibrate implementation to achieve the optimal amount of litigation. The measures are described to be agnostic as to the particular liability regime or standard of care imposed on vendors.

1. Invalidate waivers of subrogation.
Waivers of subrogation in software contracts represent a major barrier to cyber subrogation. End users are free to negotiate these out of contracts, but in practice, firms, particularly small and medium-sized enterprises, lack awareness and negotiating power. These waivers of subrogation prevent insurers bringing claims on behalf of policyholders, which could create disputes between insurer and policyholder that function to reduce vendor accountability. Invalidating waivers of subrogation allows insurers to help enforce the liability regime.

[13] Cormac Herley and Paul C. Van Oorschot, "SoK: Science, Security and the Elusive Goal of Security as a Scientific Pursuit," *Proceedings of the Symposium on Security and Privacy* (IEEE, 2017), 99–120; Daniel W. Woods and Rainer Böhme, "SoK: Quantifying Cyber Risk," *IEEE Symposium on Security and Privacy, Oakland, California,* 2021, pp. 909–26.

[14] Daniel W. Woods and Sezaneh Seymour, "Evidence-Based Cybersecurity Policy? A Meta-Review of Security Control Effectiveness," *Journal of Cyber Policy* (2024), 1–19. doi:10.1080/23738871.2024.2335461.

2. Ignore insurance payouts when setting monetary awards.
The liability of software vendors should not be reduced when customers show foresight in buying cyber insurance. This motivates the collateral source rule, which makes evidence about alternative sources of compensation, such as insurance payments, inadmissible. Not adopting the rule would dull the incentive for vendors to secure software.

3. Clarify how insurers and their insureds share monetary awards.
Various rules exist for how awards should be shared. These can be ordered from the least to most pro-subrogation: (1) no subrogation; (2) "made whole" doctrine that prioritizes the insured's compensation; (3) made whole doctrine subject to contractual modification; (4) first-dollar recovery that prioritizes the insurer's compensation; and (5) full subrogation, in which the insurer receives the entire award. While the second and third rules are typically adopted, the case for the final two rules is stronger for cyber litigation because the insureds are typically firms that suffered an economic loss, not an individual who suffered bodily injury or mental anguish, and also because deterring insecure software development is a public policy goal.

2. THE PROPOSAL

Given that subrogation involves "stepping into the shoes" of the policyholder to seek damages, a necessary requirement for this proposal is that firms can recover nonnegligible damages from vendors in relation to a failure to prevent a security incident. The precise form of that liability regime is still unclear. It could, for example, be created by a standalone federal law, or it could be an extension of the existing tort system. Instead of tying this article's proposal to a specific liability regime, we discuss a generic liability regime. Insurers have already shown that they can interact with a variety of regimes, including alternatives to the tort system such as workers' compensation and no-fault automobile insurance.[15]

Assuming a software liability regime is created, this proposal aims to harness insurance to achieve the twin goals of compensating victims and deterring insecure software development. The first goal is to establish cyber insurance as the initial source of compensation for security incidents. If firms anticipate receiving software liability payouts, then the liability regime would need to be designed to ensure fast decisions and payouts that compensate victims without creating loss inflation. We argue that cyber insurance is better placed to achieve both speed and cost control.[16] The rest of this section outlines the specific policy measures that could be enacted.

[15] Abraham, *The Liability Century*.

[16] Cyber insurance influences how policyholders respond to incidents. Insurers control various aspects, including which crisis response firms are hired, which services are provided, and at what price. Victim firms can access these services at pre-agreed, often discounted, rates by calling a 24/7 hotline. Daniel W Woods, Rainer Böhme, Josephine Wolff, and Daniel Schwarcz, "Lessons Lost: Incident Response in the Age of Cyber Insurance and Breach Attorneys," *Proceedings of the 32nd USENIX Security Symposium, Anaheim, California*, 2023, pp. 2259–73.

2.1 Subrogation Today

The insurance industry already offers digital insurance products for software vendors and potential victims of cyber incidents. Technology vendors and information technology (IT) consultants buy a policy, Tech E&O, that covers liability from errors in the provision of technology products and services, which would likely cover claims under the liability regime. Figure 1 shows that Tech E&O policies could cover software liability in various forms, be it a negligence-based tort regime or implied warranty under a product liability regime.[17]

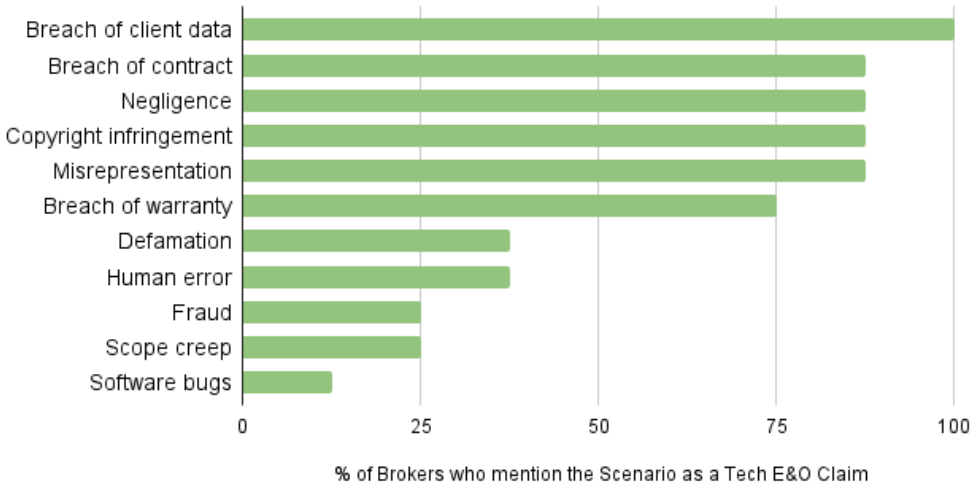

Figure 1: Scenarios used to explain potential Tech E&O claims. Breach of client data would be covered under a cyber policy, highlighting the blurred line between cyber and Tech E&O.

On the potential victim side, many businesses buy cyber insurance policies that are specifically designed to cover costs associated with cyber incidents.[18] This means there is historical data and established practice regarding how to quantify the harms associated with insecure software.[19] These costs typically include losses such as lost income, crisis response fees, and ransoms paid, as well as third-party costs such as legal defense and settlement.[20]

[17] Tech E&O insurance does not cover intentional acts like fraud or criminal activity, and it is unusual for it to cover product liability claims if the policyholder's product causes injury or property damage.

[18] Sasha Romanosky, Lillian Ablon, Andreas Kuehn, and Therese Jones, "Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?" *Journal of Cybersecurity* 5, no. 1 (2019).

[19] This includes actuarial estimates of the frequency and size of costs associated with hiring crisis response consultants, lost profits due to business interruption, litigation defense and settlement, and so on. Quantifying the mediating role of software security is less well understood.

[20] The economic losses may be difficult to recover via the tort system. Jeffrey L. Goodman, Daniel R. Peacock, and Kevin J. Rutan, "A Guide to Understanding the Economic Loss Doctrine," *Drake Law Review* 67 (2019): 1.

Despite the existence of both cyber and Tech E&O products, cyber insurers typically pay claims without seeking to subrogate and recover costs from the vendors whose insecure products caused the underlying incidents. One barrier to subrogation is that policyholders accept contracts with limitations on liability and waivers with respect to subrogation. Waivers of subrogation prevent cyber insurers from bringing a claim on behalf of policyholders, while limitations on liability mean the benefit of subrogation in terms of monetary award is small or even nonexistent.

A rare example of cyber subrogation is provided by *Ace American Insurance Co. v. Accellion, Inc.*[21] The insurer subrogated against a policyholder's service provider, Accellion, which the insurer held was responsible for the policyholder's claim[22], including a $2 million ransom and $375,000 in expenses and attorney fees.[23] Accellion's cross-suit claimed its liability was limited to the fees paid by the customer, which totaled around $42,000.[24] Ultimately, the case was settled with no money changing hands.

This case highlights various problems for cyber subrogation. First, many policyholders waive subrogation rights in service-level agreements. Second, it is difficult to prove the service provider was negligent. Third, the potential liability can be capped by the fees paid to the service provider, which means the insurer gains little from subrogation. The status quo means that end users pay higher cyber premiums to account for insecure software, while vendors face lower Tech E&O premiums than would be the case in a world with more cyber subrogation.[25]

2.2 Invalidate Waivers of Subrogation

This proposal relies on insurers seeking redress from vendors on behalf of policyholders. Many software contracts include clauses that waive the rights of insurers to do so. Waivers of subrogation are included by vendors precisely because vendors fear insurers' (and other third-parties') ability to bring claims against them. Insurers are formidable litigants because they are willing to invest resources to fight cases to establish precedent, employ teams of attorneys to understand regulations, and can systematically collect evidence from incidents suffered by multiple firms.[26] These waivers undermine the deterrent aspect of any future software liability regime that relies on private actions.[27]

---

[21] *Ace American Insurance Co. v. Accellion, Inc.* N.D. Cal., Docket No. 21-cv-9615.

[22] The complaint alleges that Accellion was negligent in not notifying the policyholder about vulnerabilities in Accellion's file transfer solution.

[23] Judy Greenwald, "No Money Changing Hands in Chubb Ransomware Settlement," Business Insurance (2022).

[24] This amount was less than 2 percent of what the insurer sought in the original lawsuit, namely $2.4 million plus interest and costs.

[25] The relevant counterfactual is a world in which Tech E&O premiums are higher to cover the risk that an insurer brings and wins a subrogated case. This would reduce the cost of cyber insurance if the amounts recovered meaningfully offset claims paid out.

[26] Abraham, *The Liability Century.*

[27] This would not be true if a public entity enforces the regime.

For insurers to subrogate, policymakers need to either rely on market forces to remove waivers or directly invalidate the waivers via legislation. We argue that the market approach is inferior. First, there is little chance that end users will unilaterally negotiate to preserve their insurers' rights when end users do not negotiate to protect their own. Second, insurer efforts to incentivize the removal of these clauses would create friction between insurers and policyholders.[28]

The market option is for policyholders to negotiate to preserve the insurer's right of subrogation. This is unlikely given that customers already sign away their own rights via limitations of liability and similar provisions in end-user licensing agreements (EULAs), largely due to the vendors' market power.[29] For example, software contracts "often dedicate a considerable portion of the EULA to disclaiming and limiting remedies and liabilities."[30] As a result, it is hard to see why customers would voluntarily fight for their insurers' rights.

The second option is for insurers to create incentives for policyholders to remove waivers from software contracts. Insurers have options in creating these incentives. Insurers could analyze the policyholders' service agreements upon application, offering favorable terms when subrogation rights are not waived. This approach avoids insurance disputes. However, both insurers and insureds must invest time in locating and analyzing all software agreements, which may not be cost-effective for low-premium policies.[31] It also creates a potential dispute if the insured fails to share a contract with a subrogation waiver, and that vendor's software goes on to cause an incident.

A simpler approach for insurers is to include cooperation clauses in cyber insurance policies. These clauses would require policyholders to retain subrogation rights and could be used to invalidate coverage if the policyholder waives subrogation rights. The core problem with this approach is that less sophisticated buyers are not aware of the requirements in their cyber insurance policy when they negotiate with vendors.[32] In such cases, software contracts would

[28] These costs manifest as both infrequent high-cost disputes, and frequent low-cost document exchange and review, as well as the insured's loss of time and other resources in negotiating such clauses. While these costs may be accepted for large insureds where a sophisticated broker is the intermediary, the cost is unlikely to be rational for small businesses where friction may prevent a sale.

[29] Nancy S. Kim, "The Software Licensing Dilemma," *BYU Law Review* (2008): 1103; Michael L. Rustad, "Software Licensing: Principles and Practical Strategies," *Suffolk University Law School Research Paper No. 14-5* (Oxford University Press, 2010).

[30] Florencia Marotta-Wurgler, "What's in a Standard Form Contract? An Empirical Analysis of Software License Agreements," *Journal of Empirical Legal Studies* 4, no. 4 (2007): 677–713.

[31] The market is stratified in that large companies engage sophisticated brokers who can afford the time to review documents and negotiate key terms. Smaller companies are typically charged smaller premiums, and brokers, who are paid on commission, have less time to spend collecting and reviewing documents. For small and medium-sized enterprises, the application process can be as simple as sharing a few pieces of information (revenue, industry, and domain) and receiving an automated quote from the insurer.

[32] This could be because they negotiated the contract before they purchased insurance or because the broker did not have time to explain the fine print of the policy or these explanations were forgotten.

contain subrogation waivers. Insurers would then face a dilemma between accepting noncooperation or enforcing the clause, which creates bad will with the insured and their broker.

Following this line of argument, one could identify and evaluate many more hypothetical strategies by which insurers could incentivize the removal of subrogation waivers. It is perhaps better to study the history of insurers creating incentives in other insurance markets, which ties into the idea of "insurance as governance."[33] Broadly speaking, researchers find that while insurers create incentives in some situations, they fail to do so in others. Incentives that create friction are particularly difficult for cyber insurance where the buyers' market has reduced insurers' market power.[34]

In summary, it is unlikely insurers will create incentives for policyholders to remove subrogation waivers. It could fail because insurers prioritize incentivizing other risk measures like security controls, or simply because insurers lack the market power to incentivize anything given the over-supply of cyber insurance. Even if incentives were created, they are unlikely to be fully effective. The remaining waivers could result in disputes between insurer and insured. For these reasons, we recommend that the software liability regime invalidate waivers of subrogation in end-user agreements, which predominantly serve the interest of vendors in avoiding accountability.

2.3 Collateral Source Rule

Our first consideration (see Section 2.2) ensures that insurers have the right to subrogate. However, it remains possible that the potential gain in terms of monetary awards is not worth the cost of subrogating. Clauses that limit liability need to be addressed. This can be seen in the aforementioned case where an insurer subrogated against a software provider, only for the vendor to claim liability was limited to the service fees.[35] We assume that other authors will address setting nonnegligible monetary awards. Instead, this proposal focuses on the potential for insurance to reduce monetary awards.

---

[33] Richard Victor Ericson, Aaron Doyle, and Dean Barry, *Insurance as Governance* (University of Toronto Press, 2003); Kenneth S. Abraham and Daniel Schwarcz, "The Limits of Regulation by Insurance," *Indiana Law Journal* 98 (2022): 215; Tom Baker and Anja Shortland, "The Government Behind Insurance Governance: Lessons for Ransomware," *Regulation & Governance* 17, no. 4 (2023): 1000–20; Tom Baker and Sean J. Griffith, "The Missing Monitor in Corporate Governance: The Directors' and Officers' Liability Insurer," *Georgetown Law Journal* 95 (2006): 1795; Omri Ben-Shahar and Kyle D. Logue, "Outsourcing Regulation: How Insurance Reduces Moral Hazard," *Michigan Law Review* 111 (2012): 197.

[34] Daniel W. Woods and Tyler Moore, "Does Insurance Have a Future in Governing Cybersecurity?" *IEEE Security & Privacy* 18, no. 1 (2020): 21–27; Josephine Wolff, *Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks* (MIT Press, 2022); Jamie MacColl, Jason R. C. Nurse, and James Sullivan, "Cyber Insurance and the Cyber Security Challenge," Royal United Services Institute, June 28, 2021; Shauhin Talesh and Bryan Cunningham, "The Technologization of Insurance: An Empirical Analysis of Big Data and Artificial Intelligence's Impact on Cybersecurity and Privacy," *Utah Law Review* (2021).

[35] Greenwald, "No Money Changing Hands in Chubb Ransomware Settlement."

One could argue that the liability regime need not compensate losses that have already been compensated by insurance. By this logic, the wrongdoer could reduce the monetary award by presenting evidence the victim had been paid by the insurer, possibly even reducing it to zero in the case of full insurance. In the software setting, vendors would face less liability because the victim independently purchased insurance, not because the vendor had built more secure software. If all victims purchased full insurance coverage, then the vendors would face no liability risk whatsoever. While this is consistent with the goal of compensating victims, such a situation would thwart the goal of improving software security.

The collateral source rule prevents insurance payouts from eroding compensation under the liability regime. It does so by making evidence inadmissible if it concerns insurance payments and other collateral sources. An example in which the collateral source rule was not applied is the September 11th Victim Compensation Fund (VCF). VCF payments were reduced if the victim's family had already received a life insurance payment. This differed from the typical tort approach of not considering life insurance payouts.[36] Recognizing alternative sources makes sense if the liability regime only aims to adequately compensate victims in the most efficient way. This was the case post-9/11 given that the airlines, rather than the wrongdoers, the terrorists, were being held liable. Compensation is unnecessary if insurance has already covered the damage.[37]

Software liability is starkly different in that deterring risky practices is an important policy goal. This goal would be undermined if insurance payments reduced monetary awards under the software liability regime. The collateral source rule prevents this problem. However, this raises the potential for double compensation, once by insurance and once by the liability regime. The insurer receiving a share, possibly all, of the liability award can prevent double compensation.

2.4 Sharing Monetary Awards

When the insurer subrogates against the software vendor, the policyholder's loss event is the basis for setting the monetary award, and their insurance policy would be ignored according to the collateral source rule. This raises the question of how the insurer and insured share this award. It is simple when the insurance indemnity payment compensates the entire loss. In this case, the insurer would receive the entire award, regardless of what it is, to uphold the indemnity principle and prevent the insured from being compensated twice.[38] In effect, this means a liable vendor would pay some (possibly all) of the victim's insurance claim, and the insurer would pay the rest.

[36] Abraham, *The Liability Century*.

[37] Given that the damage is lost life, this line of reasoning may be seen as callous.

[38] This principle holds that the maximum payout should be no greater than the loss suffered by the insured. This avoids perverse situations in which the victim prefers to suffer an incident, which can create moral hazard.

It becomes more complicated when the policyholder is not fully compensated by either the liability regime or their insurance policy. The monetary award can be less than the total loss either because the vendor is held partially liable or because the maximum amount recovered from the vendor's liability policy is less than the total loss.[39] Similarly, incomplete insurance coverage results from the loss exceeding the policy limit or coverage gaps. In these cases, the liability award must be shared in such a way that one (or both) of the insured and insurer incurs some of the loss.

Various rules exist that determine the relative priority of the insurer and insured in sharing a split subrogation award. These can be ordered from the insurer receiving lowest to highest priority: (1) no subrogation; (2) the "made whole" doctrine that prioritizes the insured's compensation; (3) the made whole doctrine subject to contractual modification; (4) first-dollar recovery that prioritizes the insurer's compensation; and (5) full subrogation, in which the insurer gets the entire award. This is a non-exhaustive list, but it tries to cover the most common rules, in practice and in theoretical discussions.

The first rule, no subrogation, says that the insurer should not receive any monetary award. This has the same effect as banning subrogated claims. The second and third rules are based on the "made whole" doctrine, which holds that the policyholder needs to be made whole for their loss before the insurer receives any share. Some states allow the rule to be modified by the terms of the insurance policy (the third rule), whereas other states do not (the second rule).[40] The fourth rule, first-dollar recovery, says the monetary award should first compensate the insurer before compensating the insured. Notably, the insured would still receive the indemnity payment under the insurance contract. Finally, full subrogation sees the insurer receive the entire monetary award from the liability regime. It has been proposed by legal scholars but has not been enacted in practice.[41]

The rules are motivated by different concerns. The made whole doctrine emphasizes compensating victims for their loss, which appeals directly to common-sense notions of what is equitable and fair. The first-dollar rule instead emphasizes upholding the contractual agreement between insurer and insured, in which the insured knowingly bore the risk of losses above the limit of the policy. In this framing, the insurer agreed to pay the first part of the loss (less the deduction/self-insured retention), and a partial liability award should correspond to that first part of the loss. First-dollar recovery places more priority on contract over equity, relative to the made whole doctrine.

---

[39] Section 3.1.1 discusses the problem of shared responsibility in more detail. In practice, this could be solved via several liability, in which a vendor was held liable for only a percentage of the loss.

[40] Hart, "The Myth of the Superlien."

[41] Jeffrey O'Connell, "Transferring Injured Victims' Tort Rights to No-Fault Insurers: New Sole Remedy Approaches to Cure Liability Insurance Ills," *University of Illinois Law Forum* (1977): 749; Robert Cooter, "Towards a Market in Unmatured Tort Claims," *Virginia Law Review* (March 1989): 383–411; Stephen Marks, "The Market in Unmatured Tort Claims: Twenty-Five Years Later," *Pace Law Review* 34 (2014): 185.

Full subrogation prioritizes the insurer, much like first-dollar recovery, but it is typically motivated by economic efficiency. It seeks to address the principal-agent problem when insurers control the legal claim but do not receive the whole award. This can result in under-deterrence, such as when insurers settle tort suits for a monetary amount that covers the insurer's claims costs but do not push for greater monetary awards.[42] As such, full subrogation appeals to the goal of holding wrongdoers accountable for their actions.

The importance of each goal—compensating the victim, upholding the contract, or deterring the wrongdoer—varies by the type of liability. The made whole doctrine's focus on compensation is perhaps most compelling in cases where a victim has suffered injury and mental anguish. Indeed, Maher and Pathak open an article about tort subrogation with a *Wall Street Journal* story in which the accident settlement was not sent to the victim, who was left permanently brain damaged and in a wheelchair following the accident.[43] Tort reformers face an uphill battle arguing that insurers hold priority in settings where victims regularly suffer bodily and psychological harm.

In contrast to, say, automobile accidents, the main harms for software liability are financial losses—lost profits; money to pay a ransom, pay crisis responders, or settle a lawsuit—that show up on the company's balance sheet. While these parties still need compensation, the need is less salient than for individual victims of physical injury. This suggests a pro-subrogation rule is less objectionable for software liability than in other areas. The goal of deterring the wrongdoer is also more salient for software liability, to the extent software vendors are under-deterred at present. Insurers would be more motivated to use subrogation and hold vendors accountable if they received a greater share of the reward. The political issue is perhaps less thorny given that victims typically cannot recover claims from software vendors in the status quo anyway, so victims would not lose a benefit if a rule that favored the insurer was introduced.[44] For these reasons, we believe a pro-subrogation rule, perhaps first-dollar recovery, could be appropriate for software liability.

2.5 Summary

These pro-subrogation measures aim to improve the liability regime's enforcement power by harnessing insurers' legal resources and information advantage in bringing claims against vendors of insecure software. The first measure is to invalidate waivers of subrogation. Widespread waivers would thwart the enforcement power of insurers. It is unlikely that market forces will remove these, given that most users already negotiate away their own legal rights to recover from vendors.[45] For these reasons, we believe invalidating these clauses is in the public interest and should not be left to imperfect market forces.

---

[42] Abraham, *The Liability Century*.

[43] Brendan S. Maher and Radha A. Pathak, "Understanding and Problematizing Contractual Tort Subrogation," *Loyola University of Chicago Law Journal* 40 (2008): 49.

[44] Marotta-Wurgler, "What's in a Standard Form Contract?"; Rustad, "Software Licensing."

[45] Kim, "The Software Licensing Dilemma"; Rustad, "Software Licensing."

The second component, the collateral source rule, prevents cyber insurance from dulling the incentives created by software liability. Without such a rule, monetary awards would be reduced as a result of victims showing foresight in buying cyber insurance. Double compensation would not be an issue as insurers can use subrogation rights to recover claims paid out. In effect, this means vendors pay a proportion of the cyber insurance claim.

We argued that in the case of a split subrogation award, there is a stronger case for a pro-subrogation rule like first-dollar recovery than there is for other lines of insurance. Given that many states allow insurance policies to deviate from the made whole doctrine even in insurance lines where bodily injury is common, it seems there is room to deviate for software liability. This is especially true given that policymakers believe insecure software development is under-deterred at present, and a pro-subrogation rule supports accountability.[46]

3. ANTICIPATED OUTCOMES

One overarching question is whether these measures will actually lead insurers to subrogate. The question arises because there have been so few successful cases of insurers subrogating against vendors to date. Indeed, insurers face substantial barriers to subrogation in any insurance line.[47] Yet cyber subrogation was still attempted in spite of general challenges and also software-specific issues like widespread limitations of liability and subrogation waivers.[48] Broadening software liability and enacting pro-subrogation measures (as described in Section 2) would make these attempts more frequent, although we cannot say how frequent.

With this in mind, we proceed by evaluating the impact of a nonnegligible increase in the rate of cyber subrogation. Each subsection focuses on the impact on businesses, secure software development, the insurance industry, and the legal system at large. We first focus on the liability regime, as this has follow-on effects for the other stakeholders.

3.1 Liability Regime

To evaluate how cyber subrogation impacts the functioning of the liability regime, we need to compare how insurers would bring claims relative to individual firms or a class-action suit. The main differences lie in the evidence insurers can collect, and their ability to craft legal strategies

[46] The White House, *National Cybersecurity Strategy.*

[47] A non-exhaustive list includes (1) subrogation is expensive; (2) the outcome is uncertain; (3) strained customer relationships because (a) subrogation requires an external organization (the insured) to cooperate in sharing evidence even though they have little interest in the outcome and (b) insureds may not want their insurers to subrogate as it damages relationship with vendors; (4) the benefits of subrogation often do not arise until the conclusion of a multi-year court case, which complicates projecting and reporting on loss ratios; (5) judges and juries are not typically sympathetic to insurers in legal cases; and (6) the insurer may have insured both the injured party and the wrongdoer.

[48] Greenwald, "No Money Changing Hands in Chubb Ransomware Settlement."

across multiple cases. In particular, the homogeneity of software across firms gives rise to the potential for subrogated class-action suits coordinated by an insurer.[49]

3.1.1 Evidence

Insurers can collect and present unique evidence that addresses two core issues with assigning fault in the context of cybersecurity: (a) the stochastic nature of security incidents and (b) joint responsibility. Given that 100 percent security while maintaining modern functionality is impossible, security incidents caused by software exploits are inevitable.[50] The regime cannot punish all incidents and must instead focus on whether the vendor has showed prudence in preventing incidents. Some proposals aim to affirmatively define a standard of care, which would qualify the vendor for a safe harbor if followed.[51]

Insurers can instead provide outcome-focused evidence about the relative rates of compromise associated with different software solutions. For example, suppose claims data shows that organizations with Internet-exposed software from a specific vendor were three times more likely to suffer a claim.[52] It is both illustrative and naive to interpret this evidence as causal. In the causal interpretation, firms have a baseline likelihood of a security incident, and adopting specific solutions makes this three times as likely. If that vendor has also failed to meet the standard of care, this actuarial evidence would strengthen the case that the vendor has not shown enough prudence or caution in securing the product.

The problem is we cannot interpret this evidence causally. This is partly because there is joint responsibility in securing modern networks. Firms deploy various software solutions, multiple of which could be at fault. This is unlike workers' compensation where the accident occurred at one workplace, which identifies a clear employer that should be held liable. End users also have considerable agency in designing and managing networks, which includes implementing security controls and processes. This is unlike, say, pollution liability, where the victim cannot control where a company dumps toxic waste.

Vendors and end users are jointly responsible for preventing security incidents. Software vendors should implement reasonable secure software engineering practices to avoid obvious design flaws, but software adopters must also architect networks and manage security processes. A further complexity is that the relative responsibility will vary by product.[53]

---

[49] This would not work for auto or medical malpractice liability because one single driver or doctor can impact only so many individuals, whereas the same software solutions are rolled out across thousands of businesses. See Carl Shapiro and Hal R. Varian, *Information Rules: A Strategic Guide to the Network Economy* (Harvard Business Press, 1998).

[50] Ross Anderson, *Security Engineering* (Wiley, 2008).

[51] Dempsey, "Standards for Software Liability."

[52] Coalition. 2023 Cyber Claims Report. https://info.coalitioninc.com/download-2023-cyber-claims-report.html.

[53] There is less reason for a human resource (HR) system to be exposed to the internet as compared with a virtual private network. For HR systems, risk may be mitigated more efficiently by end users segmenting the system from

Network boundary device vendors might have more responsibility to eliminate vulnerabilities than do human resource system vendors. A similar argument about joint responsibility for creating and applying software patches can be made.[54]

Statistical evidence provided by insurers can also help untangle joint responsibility. Returning to the earlier example, claims data showed that organizations with a specific VPN client were three times more likely to suffer a claim.[55] One could argue that the vendor is responsible for two-thirds of the costs of incidents, namely the share of the risk that is elevated above the baseline by adopting the product. Directly assigning liability in line with these statistics is naive because of potential confounding variables; however, it illustrates the potential for actuarial evidence to untangle the question of joint responsibility.[56]

This kind of statistical evidence is not available for either individuals or a group of individuals in a class-action lawsuit because all the parties to the suit would have adopted the vendor's technology. In the language of experimental design, these class-action suits lack a relevant control group. In contrast, insurers have many control groups, provided there is variation in the software deployed by their policyholders. This evidence can help untangle the thorny issue of joint responsibility.

3.1.2 Legal Strategies

Insurers exhibit considerable control over liability litigation, both in defending the liable party and in subrogating on behalf of the injured party.[57] In doing so, insurers employ teams of attorneys to develop optimal legal strategies. This involves deciding when to settle out of court and save on lawyers' fees, and when to invest in pursuing an uncertain case to win a large monetary award or establish precedent. It is difficult to anticipate how these competing goals will play out, but we can at least outline how insurers approach legal strategies, compared to an individual vendor or customer.

For individual victims, monetary awards are a consistent upside (and a downside for individual vendors). Legal fees are necessary to bring a potential gain (or mitigate a potential loss). Insurers differ in that the monetary award can be a negative or a positive depending on which side of the liability case the insurer is on. This is particularly true for software liability given that

---

the internet than it would by the vendor building in security. In contrast, networking software, such as a software firewall, can function only if it is exposed to the internet, and so adopters cannot pursue segmentation.

[54] A vendor that sits on a vulnerability report for months before issuing a patch is more responsible than a vendor that promptly releases a patch. Similarly, a software adopter that does not apply a patch for months is more responsible for a security incident than one that patched within a week of release.

[55] Coalition, 2023 Cyber Claims Report.

[56] Samaneh Tajalizadehkhoob et al., "Herding Vulnerable Cats: A Statistical Approach to Disentangle Joint Responsibility for Web Security in Shared Hosting," in *Proceedings of the Conference on Computer and Communications Security* (Association for Computing Machinery, 2017), 553–67.

[57] Abraham, *The Liability Century*.

the same insurers sell cyber and Tech E&O coverage.[58] However, legal fees are a consistent downside in both cases. This creates an imperative for insurers to control lawyers' fees. In terms of how this will play out, Abraham observes that "liability insurers employ a bureaucracy that promotes routinized settlement" using "rules of thumb" that individual defendants are less likely to deploy.[59] We can expect cyber and Tech E&O insurers to deploy similar tactics, at least after consistent rules have developed.

Yet a competing logic also holds for insurers, given that they "can afford not to settle cases" and instead invest in achieving a court decision.[60] This stronger position allows insurers to pursue defendants for a full liability award, whereas an uninsured defendant may be forced to settle due to risk aversion and the lack of cash to pursue a case. As repeat litigation players, insurers can fight cases in court to establish precedents that later become routinized rules of thumb.

These competing logics—to settle and to fight in court—will play out differently over time. Initially, insurers will have no rules of thumb to settle liability cases. As such, insurers may be among the first parties to bring liability claims against software vendors. These cases could establish precedents that later become rules of thumb, allowing for more efficient out-of-court settlements in the long term.

3.2 Insurance Market

The impact of cyber subrogation depends on the frequency of successful subrogated cases and the size of the awards to the insurer. If the expected gains are negligible, then it remains possible that cyber subrogation is an infrequent windfall that "plays no part" in pricing or coverage.[61] However, a sufficiently expansive regime could lead insurers to reduce the expected cost of selling cyber insurance, given that they inherit the right to recover against vendors. All else being equal, this possibility could result in some combination of broader coverage, higher limits, and/or lower price of first-party cyber insurance. In practice, these effects could be swamped by broader market dynamics, and so this section talks about marginal effects.

A reduction in cyber insurance premiums may not be evenly spread across policyholders. In the status quo, a firm implementing insecure software products is more likely to face a claim and

[58] Given that large limits for Tech E&O require a tower policy, it could be the case that multiple insurers are exposed to a software liability case against the vendor. This would disincentivize those insurers subrogating on behalf of their cyber policyholders, as they would essentially bring a claim against themselves (depending on whether the award touches their part of the tower). However, insurers not in the tower may face additional incentive to bring a claim given that it would negatively impact competitors. It is difficult to anticipate how these dynamics would play out.

[59] Abraham, *The Liability Century*.

[60] Ibid.

[61] Edwin Wilhite Patterson, *Essentials of Insurance Law* (McGraw-Hill, 1957), 151.

pay a higher premium.[62] The liability regime reduces the increased risk associated with insuring such firms. Although firms deploying insecure solutions are more likely to suffer a claim, the insurer is also more likely to be able to recover claims costs by subrogating against the vendor. This suggests that the marginal reduction in cyber insurance prices will be steepest for firms that have adopted insecure software, even if pricing schemes do not immediately account for this.[63] This is not necessarily a bad outcome given that most firms lack the security expertise to identify secure software.[64]

Turning to Tech E&O, a consequential increase in cyber subrogation would increase the risk of vendors being held liable. Software vendors would be punished via higher liability insurance prices, all else being equal. Price increases would be highest for vendors of insecure software, again assuming rational pricing with perfect information. Insurers would assess software security by collecting information via audits, questionnaires, and so on.

The danger, however, is that an overly punitive liability regime leads to steep Tech E&O price hikes and insurers withdrawing coverage. This was the case for pollution liability where insurers excluded coverage from commercial general liability policies.[65] The market for software, in which identical products are adopted by many customers, creates the potential for correlated monetary awards that would undoubtedly scare insurers.[66] Managing this potential issue is not addressed—and is actually made worse—by this proposal because increased cyber subrogation increases the likelihood of Tech E&O claims.

We now turn to how these changes in the insurance market flow through to software vendors and users.

3.3 Software Vendors

A sufficiently broad and punitive software liability regime would mean vendors pay more for Tech E&O insurance, but this is not specific to this proposal. We propose making insurers central to the liability regime. Vendors would be exposed to higher litigation risk due to subrogated actions, which is why software contracts include waivers of subrogation at present. However, insurance could also benefit vendors by limiting ex post moral hazard and controlling legal costs. The cost of incident response (IR) is likely to influence the monetary awards, but the

[62] This assumption of actuarially fair pricing is arguably too strong due to the current state of cyber actuarial science. However, cyber actuaries have identified some software solutions that are associated with higher risk, which is baked into pricing.

[63] Romanosky et al., "Content Analysis of Cyber Insurance Policies."

[64] Ross Anderson and Tyler Moore, "The Economics of Information Security," *Science* 314, no. 5799 (2006): 610–13.

[65] Abraham, *The Liability Century*.

[66] Kenneth S. Abraham and Daniel Schwarcz, "Courting Disaster: The Underappreciated Risk of a Cyber Insurance Catastrophe," *Connecticut Insurance Law Journal* 27 (2020): 407; Dan Geer, Eric Jardine, and Eireann Leverett, "On Market Concentration and Cybersecurity Risk," *Journal of Cyber Policy* (2020): 1–21.

victim chooses which IR firms and services to hire.[67] This principal-agent problem could lead to inflation in response costs, which is detrimental to vendors. Insurers address this ex post moral hazard by controlling how policyholders respond to cyber incidents, which involves negotiating hourly rates and choosing which firms to hire.[68] Insurers also help reduce costs of the liability regime by creating a system with clear rules for settlements.

An uncertain impact is whether insurers create incentives for vendors to improve software security. The underlying logic is that insurers will assess software development practices and offer discounts and subsidies for more secure practices.[69] If the liability regime contains a safe harbor, then insurers would assess whether the vendor has implemented the required standard of care. However, we caution readers against overemphasizing this positive role of insurers given that it requires a combination of market conditions and knowledge of risk that is not always present.[70] To understand this better, empirical studies of the Tech E&O market should evaluate how it impacts the security practices of software vendors and IT consultants.

3.4 Software Users

We consider policyholders and non-policyholders separately.

3.4.1 Policyholders

In exchange for giving subrogation rights to their cyber insurer, policyholders could receive the immediate benefit of improved insurance coverage and/or a lower price. Users benefit from rapid compensation given that insurance claims are typically resolved much sooner than, say, liability claims, which take years to resolve in a tort system. Some insurers even offer "pay-on-behalf of" policies, in which the insurer fronts the cash for crisis response services.[71]

Insurers subrogating also smooths risk for firms. At best, a liability regime provides the same function of insurance in compensating victims for their loss. However, the liability regime is likely to be inconsistent. A vendor's software might be insecure enough to cause an incident but not insecure enough to trigger the threshold for a liability case. A case might also be rejected due to a lack of evidence. Such cases leave victims with a loss caused by insecure software but no compensation. Insurance mitigates this by pooling the risk of no compensation across policyholders given that insurance pay-outs are not linked to the liability of the software vendor. Admittedly, this function comes at the cost of firms having to pay an insurance premium.

---

[67] This might involve negotiating an expensive rate, or consuming unnecessary services.

[68] Woods et al., "Lessons Lost."

[69] Ben-Shahar and Logue, "Outsourcing Regulation."

[70] Ericson, Doyle, and Barry, *Insurance as Governance*; Abraham and Schwarcz, "The Limits of Regulation by Insurance"; Baker and Shortland, "The Government Behind Insurance Governance"; Baker and Griffith, "The Missing Monitor in Corporate Governance."

[71] Rob Thoyts, *Insurance Theory and Practice* (Routledge, 2010).

A more subtle benefit of this proposal is preventing friction between policyholders and their insurers. Insurance policies may include cooperation clauses that require policyholders to preserve the insurer's right to subrogate. Inevitably some firms will fail to do so, which can lead to an insurance dispute. Invalidating waivers of subrogation helps to avoid this situation.

3.4.2 Non-Policyholders

A natural question is how this proposal impacts firms that choose not to purchase insurance. Although the bulk of the benefits flow to policyholders, non-policyholders could still benefit from the legal strategies and evidence brought by insurers. As already discussed, insurers are well placed to invest in early legal cases, thereby establishing precedent. Actuarial evidence used to prove that a specific vendor is liable could be reused by non-policyholders. For these reasons, it is unclear that non-policyholders lose out from this proposal.

4. CONCLUSION

This proposal takes advantage of the reality that insurance will intermediate any future software liability regime, as it has for various U.S. liability regimes since the nineteenth century.[72] Many technology vendors already purchase software liability insurance (Tech E&O) that covers errors and omissions—including security failures—in the provision of technology products and services. Many end users purchase cyber insurance that provides compensation for incidents caused by insecure software. In effect, insurance shields vendors from liability and provides an alternative source of compensation for end users.

The first aim of this proposal is to allow insurers to bring claims under the software liability regime on behalf of policyholders. This harnesses insurers' comparative advantage in formulating a legal strategy, funding legal proceedings, and collecting relevant evidence. For insurers to bring claims under the regime, the regime should invalidate waivers of subrogation in software contracts, the first plank of the proposal.

The second part of the proposal addresses the problem of first-party insurance and the liability regime competing as sources of compensation. Vendors could avoid accountability by arguing that the end user's cyber insurance policy has already compensated the victim. We recommend the software liability regime makes such evidence inadmissible. This rule is known as the collateral source rule. When combined with the first part of the proposal, enacting this rule would allow insurers to subrogate against vendors to recover cyber insurance claims costs. Some of the benefits of insurers recovering claims costs from vendors would flow back to policyholders in the form of cheaper insurance and/or broader coverage.

The final part of this proposal discusses how split subrogation awards should be shared between insurer and insured. We outlined the competing goals at play—compensating the

[72] Abraham, *The Liability Century*.

victim, upholding the insurance contract, and deterring insecure software—and argued that compensating victims is comparatively less important given that most software losses are economic, and deterrence is comparatively more important in light of the U.S. National Cybersecurity Strategy.[73] With this in mind, it could make sense to adopt the first-dollar recovery rule for software liability. This will incentivize insurers to bring subrogated claims and would help spread losses across policyholders if subrogation materially impacts loss ratios.

To conclude, considering insurance while formulating the software liability regime can accomplish a number of desirable policy goals. The regime will more reliably achieve justice when insurers test legal arguments supported by actuarial evidence about the relative responsibility of end users and software vendors. Over time, insurers can develop cost-efficient rules of thumb to avoid costly legal proceedings. This would mean a greater share of liability payments go toward compensating victims. As such, end users may receive better insurance coverage, allowing rapid compensation without having to navigate the liability regime.

[73] The White House, *National Cybersecurity Strategy*.